IN THE CLAIMS

Kindly amend claims 1, 2, 25 and 26, cancel claims 16, 17, 34 and 35, and add new claims 45-48 as follows.

The following is a complete listing of revised claims with a status identifier in parenthesis.

LISTING OF CLAIMS

1. (Currently Amended) A method for use in a system which includes a cryptographic key store for storing a transformed cryptographic key and accessing circuitry for accessing the transformed cryptographic key from the cryptographic key store, the method comprising the step of:

storing key re-transforming information for the transformed cryptographic key in a decryption store, the accessing circuitry ~~being able to communicate~~ communicating with the decryption store ~~exclusively~~ via ~~a predetermined~~ an address-limited port that includes an interface, the interface preventing the port from addressing at least portions of ~~being such that the accessing circuitry is unable to access from the decryption store~~ at least one of: a) ~~at least a portion of the~~ key re-transforming information, and b) ~~at least~~ a ~~portion of the~~ cryptographic key;

wherein said key re-transforming information ~~has a~~ comprises a randomly generated transformation pattern ~~randomly generated by said decryption store~~.

2. (Currently Amended) The method of claim 1 wherein the interface further prevents the port from addressing at least portions of ~~is such that the accessing circuitry is unable to access from the decryption store~~ both ~~of: a) at least a portion of~~ the key re-transforming information, and ~~b) at least a portion of~~ the cryptographic key.

3. (Previously Presented) The method of claim 1 wherein the key re-transforming information further comprises a key decrypting algorithm.

4. (Original) The method of claim 3 wherein the transformation pattern comprises a unique identifier of the decryption store.

5. (Original) The method of claim 1 further comprising the steps of:

the decryption store receiving the cryptographic key;

the decryption store transforming the cryptographic key using key transforming information to produce the transformed cryptographic key; and

the decryption store sending the transformed cryptographic key to the cryptographic key store.

6. (Original) The method of claim 1 wherein:

the decryption store comprises a mobile terminal;

the cryptographic key store comprises a computer memory; and the accessing circuitry comprises a processor.

7. (Original) The method of claim 1 wherein:

the decryption store comprises a network access card;

the cryptographic key store comprises a computer memory; and the accessing circuitry comprises a processor.

8. (Original) The method of claim 1 further comprising the steps of:

the decryption store receiving the transformed cryptographic key and information;

the decryption store re-transforming the transformed cryptographic key using the key re-transforming information to produce the cryptographic key;

and the decryption store encrypting the information using the cryptographic key to produce encrypted information.

9. (Original) The method of claim 8 further comprising the step of transmitting the encrypted information.

10. (Original) The method of claim 1 further comprising the steps of:

the decryption store receiving encrypted information;

the decryption store receiving the transformed cryptographic key;

the decryption store re-transforming the transformed cryptographic key using key re-transforming information to produce the cryptographic key; and

the decryption store decrypting the encrypted information using the cryptographic key to produce decrypted information.

11. (Original) The method of claim 10 further comprising the step of the accessing circuitry accessing the decrypted information.

12. (Original) The method of claim 1 wherein the accessing circuitry's communication with the decryption store comprises the transfer of information between them.

13. (Original) The method of claim 1 wherein the storing step comprises storing the transformed cryptographic key in the cryptographic key store for a period of time.

14. (Original) The method of claim 1 further comprising the step of erasing the cryptographic key from the decryption store at the completion of each cryptographic operation.

15. (Original) The method of claim 1 wherein the cryptographic key is stored in the decryption store in such a way that it disappears from the decryption store when the decryption store is removed from the system.

16. (Cancelled)

17. (Cancelled)

18. (Currently Amended) The system of ~~claim 16~~ claim 45 wherein[[:]] the decryption store comprises a mobile terminal[[;]], the cryptographic key store comprises a computer memory[[;]], and the accessing circuitry comprises a processor.

19. (Currently Amended) The system of ~~claim 16~~ claim 45 wherein[[:]]

the decryption store comprises a network access card[[;]],

the cryptographic key store comprises a computer memory[[;]], and the accessing circuitry comprises a processor.

20. (Currently Amended) The system of ~~claim 16~~ claim 45 wherein the decryption store further comprises:

an input port for receiving the transformed cryptographic key;

a key decrypting module for decrypting the transformed cryptographic key using the key re-transforming information to produce the cryptographic key;

an encrypting module for encrypting information using the cryptographic key to produce encrypted information.

21. (Original) The system of claim 20 wherein the decryption store further comprises a transmitter for transmitting the encrypted information.

22. (Currently Amended) The system of ~~claim 16~~ claim 45 wherein the decryption store further comprises:

an input port for receiving the transformed cryptographic key;

a key decrypting module for decrypting the transformed cryptographic key using the key re-transforming information to produce the cryptographic key;

a decrypting module for decrypting encrypted information.

23. (Original) The system of claim 22 wherein the decryption store further comprises a receiver for receiving the encrypted information.

24. (Currently Amended) The system of ~~claim 16~~ claim 45 wherein the decryption store further comprises:

a receiver for receiving the cryptographic key;

a key encrypting module for encrypting the cryptographic key using key transforming information to produce the transformed cryptographic key; and [[an]] wherein the output port ~~for outputting~~ outputs the transformed cryptographic key.

25. (Currently Amended) A decryption store for storing key re-transforming information for a transformed cryptographic key, the decryption store comprising:

an address-limited output port, including an ~~a predetermined~~ interface~~, the interface being operable to receive~~ that prevents the port from addressing at least portions of at least one of stored key-re-transforming information and a cryptographic key, for receiving the transformed cryptographic key~~; and~~

wherein the ~~an output port complying exclusively with the predetermined interface such that~~ information is accessible from the decryption store through the output port[[;]]

~~wherein at least one of: a) at least a portion of the key re-transforming information, and b) at least a portion of the cryptographic key being not accessible from the decryption store through the output port;~~ and ~~wherein~~ said ~~key re-transforming~~ information [[has]] comprises a randomly generated transformation pattern ~~randomly generated by said decryption store~~.

26. (Currently Amended) The ~~invention~~ decryption store of claim 25 wherein said interface further prevents the port from addressing at least portions of ~~is such that at least~~ both [[of]]: a) ~~at least a portion of~~ the key re-transforming information, and b) ~~at least a portion of~~ the cryptographic key ~~are not accessible from the decryption store through the output port~~.

27. (Currently Amended) The ~~invention~~ decryption store of claim 25 wherein the decryption store comprises a mobile terminal.

28. (Currently Amended) The ~~invention~~ decryption store of claim 25 wherein the decryption store comprises a network access card.

29. (Currently Amended) The ~~invention~~ decryption store of claim 25 wherein the decryption store further comprises:

a key decrypting module for decrypting the transformed cryptographic key using the key re-transforming information to produce the cryptographic key;

an encrypting module for encrypting information using the cryptographic key to produce encrypted information; and

a decrypting module for decrypting encrypted information.

30. (Currently Amended) The ~~invention~~ decryption store of claim 29 wherein the decryption store further comprises a transmitter for transmitting the encrypted information.

31. (Currently Amended) The ~~invention~~ decryption store of claim 25 wherein the decryption store further comprises:

a receiver for receiving the cryptographic key; and

a key encrypting module for encrypting the cryptographic key using key transforming information to produce the transformed cryptographic key.

32. (Currently Amended) The ~~invention~~ decryption store of claim 31 wherein the transformed cryptographic key is a function of a transformation pattern.

33. (Currently Amended) The ~~invention~~ decryption store of claim 32 wherein the transformation pattern comprises a unique identifier of the decryption store.

34. (Cancelled)

35. (Cancelled)

36. (Currently Amended) The method of ~~claim 34~~ claim 47 wherein the key retransforming information comprises a key decrypting algorithm.

37. (Original) The method of claim 36 wherein the transformation pattern comprises a unique identifier of the decryption store.

38. (Currently Amended) The method of ~~claim 34~~ claim 47 further comprising the steps of:

the decryption store receiving the cryptographic key;

the decryption store transforming the cryptographic key using key transforming information to produce the transformed cryptographic key; and

the decryption store sending the transformed cryptographic key to a cryptographic key store via the output port.

39. (Currently Amended) The method of ~~claim 34~~ claim 47 wherein the decryption store comprises a mobile terminal.

40. (Currently Amended) The method of ~~claim 34~~ claim 47 wherein the decryption store comprises a network access card.

41. (Currently Amended) The method of ~~claim 34~~ claim 47 further comprising the steps of:

the decryption store receiving information; and

the decryption store encrypting the information using the cryptographic key to produce encrypted information.

42. (Original) The method of claim 41 further comprising the step of transmitting the encrypted information.

43. (Currently Amended) The method of ~~claim 34~~ claim 47 further comprising the steps of:

the decryption store receiving encrypted information[[;]], and ~~the decryption store~~ decrypting the information using the cryptographic key to produce decrypted information.

44. (Original) The method of claim 43 further comprising the step of sending the decrypted information to accessing circuitry via the output port.

45. (New) A system comprising:

a cryptographic key store for storing a transformed cryptographic key;

accessing circuitry for accessing the transformed cryptographic key from the cryptographic key store;

a decryption store for storing key re-transforming information for the transformed cryptographic key,

wherein the accessing circuitry communicates with the decryption store via an address-limited output port that includes an interface, the interface preventing the port from addressing at least portions of at least one of: a) key re-transforming information, and b) a cryptographic key;

wherein said key re-transforming information comprises a randomly generated transformation pattern.

46. (New) The method of claim 45 wherein the interface further prevents the port from addressing at least portions of both the key re-transforming information and the cryptographic key.

47. (New) A method for storing key re-transforming information for a transformed cryptographic key, the method comprising:

receiving the transformed cryptographic key; and

preventing an address-limited output port, including a predetermined interface, from addressing at least portions of at least one of stored key-re-transforming information and an encryptographic key,

wherein said key re-transforming information comprises a randomly generated transformation pattern.

48. (New) The method of claim 47 further comprising preventing the port from addressing at least portions of both the key re-transforming information and the cryptographic key.